the Attorney General, shall begin implementation of the environment to enable participants in the environment to develop and run analytic tools referred to in subsection (b) on specified data sets for the purpose of identifying, mitigating, and preventing malicious cyber activity that is a threat to public and private critical infrastructure.

(B) REQUIREMENTS.—The environment and the use of analytic tools referred to in subsection (b) shall—

(i) operate in a manner consistent with relevant privacy, civil rights, and civil liberties policies and protections, including such policies and protections established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(ii) account for appropriate data interoperability requirements;

(iii) enable integration of current applications, platforms, data, and information, including classified information, in a manner that supports the voluntary integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate;

(v) ensure accessibility by entities the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, determines appropriate;

(vi) allow for access by critical infrastructure stakeholders and other private sector partners, at the discretion of the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General;

(vii) deploy analytic tools across classification levels to leverage all relevant data sets, as appropriate;

(viii) identify tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs; and

(ix) anticipate the integration of new technologies and data streams, including data from government-sponsored network sensors or network-monitoring programs deployed in support of non-Federal entities.

(3) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PROGRAM.—Not later than 1 year after the date of enactment of this Act, and every year thereafter until the date that is 1 year after the program under this section terminates under subsection (g), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives a report that details—

(A) Federal Government participation in the environment, including the Federal entities participating in the environment and the volume of information shared by Federal entities into the environment;

(B) non-Federal entities' participation in the environment, including the non-Federal entities participating in the environment and the volume of information shared by non-Federal entities into the environment;

(C) the impact of the environment on positive security outcomes for the Federal Government and non-Federal entities;

(D) barriers identified to fully realizing the benefit of the environment both for the Federal Government and non-Federal entities;

(E) additional authorities or resources necessary to successfully execute the environment; and

(F) identified shortcomings or risks to data security and privacy, and the steps necessary to improve the mitigation of the shortcomings or risks.

(d) CYBER THREAT DATA INTEROPERABILITY REQUIREMENTS.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall identify or establish data interoperability requirements for non-Federal entities to participate in the environment.

(2) DATA STREAMS.—The Secretary, in coordination with the heads of appropriate departments and agencies, shall identify, designate, and periodically update programs that shall participate in or be interoperable with the environment, in a manner consistent with data security standards under Federal law, which may include—

(A) network-monitoring and intrusion detection programs;

(B) cyber threat indicator sharing programs;

(C) certain government-sponsored network sensors or network-monitoring programs;

(D) incident response and cybersecurity technical assistance programs; or

(E) malware forensics and reverse-engineering programs.

(3) DATA GOVERNANCE.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall establish procedures and data governance structures, as necessary, to protect data shared in the environment, comply with Federal regulations and statutes, and respect existing consent agreements with private sector critical infrastructure entities that apply to critical infrastructure information.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall change existing ownership or protection of, or policies and processes for access to, agency data.

(e) NATIONAL SECURITY SYSTEMS.—Nothing in this section shall apply to national security systems, as defined in section 3552 of title 44, United States Code, or to cybersecurity threat intelligence related to such systems, without the consent of the relevant element of the intelligence community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(f) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—The Director of National Intelligence shall ensure that any information sharing conducted under this section shall protect intelligence sources and methods from unauthorized disclosure in accordance with section 102A(i) of the National Security Act (50 U.S.C. 3024(i)).

(g) DURATION.—The program under this section shall terminate on the date that is 5 years after the date of enactment of this Act.

TITLE LIII—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 5401. ESTABLISHMENT OF HIRING AUTHORITIES FOR THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the National Cyber Director.

(2) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given such term in section 2103 of title 5, United States Code.

(3) OFFICE.—The term ''Office'' means the Office of the National Cyber Director.

(4) QUALIFIED POSITION.—The term ''qualified position'' means a position identified by the Director under subsection (b)(1)(A), in which the individual occupying such position performs, manages, or supervises functions that execute the responsibilities of the Office.

(b) HIRING PLAN.—The Director shall, for purposes of carrying out the functions of the Office—

(1) craft an implementation plan for positions in the excepted service in the Office, which shall propose—

(A) qualified positions in the Office, as the Director determines necessary to carry out the responsibilities of the Office; and

(B) subject to the requirements of paragraph (2), rates of compensation for an individual serving in a qualified position;

(2) propose rates of basic pay for qualified positions, which shall—

(A) be determined in relation to the rates of pay provided for employees in comparable positions in the Office, in which the employee occupying the comparable position performs, manages, or supervises functions that execute the mission of the Office; and

(B) subject to the same limitations on maximum rates of pay and consistent with section 5341 of title 5, United States Code, adopt such provisions of that title to provide for prevailing rate systems of basic pay and apply those provisions to qualified positions for employees in or under which the Office may employ individuals described by section 5342(a)(2)(A) of such title; and

(3) craft proposals to provide—

(A) employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5, United States Code; and

(B) employees in a qualified position for which the Director proposes a rate of basic pay under paragraph (2) an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

SA 4785. Mr. OSSOFF (for himself, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. DR. DAVID SATCHER CYBERSECURITY EDUCATION GRANT PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Cybersecurity Opportunity Act''.

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) ENROLLMENT OF NEEDY STUDENTS.—The term ''enrollment of needy students'' has the meaning given the term in section 312(d) of the Higher Education Act of 1965 (20 U.S.C. 1058(d)).

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(5) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution listed in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(c) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—Subject to the availability of appropriations, the Director shall carry out the Dr. David Satcher Cybersecurity Education Grant Program by—

(A) awarding grants to assist institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to establish or expand cybersecurity programs, to build and upgrade institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities, and to support such institutions on the path to producing qualified entrants in the cybersecurity workforce or becoming a National Center of Academic Excellence in Cybersecurity; and

(B) awarding grants to build capacity at institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to expand cybersecurity education opportunities, cybersecurity programs, cybersecurity research, and cybersecurity partnerships with public and private entities.

(2) RESERVATION.—The Director shall award not less than 50 percent of the amount available for grants under this section to historically Black colleges and universities and minority-serving institutions.

(3) COORDINATION.—The Director shall carry out this section in consultation with appropriate Federal agencies.

(4) SUNSET.—The Director's authority to award grants under paragraph (1) shall terminate on the date that is 5 years after the date the Director first awards a grant under paragraph (1).

(d) APPLICATIONS.—An eligible institution seeking a grant under subsection (a) shall submit an application to the Director at such time, in such manner, and containing such information as the Director may reasonably require, including a statement of how the institution will use the funds awarded through the grant to expand cybersecurity education opportunities at the eligible institution.

(e) ACTIVITIES.—An eligible institution that receives a grant under this section may use the funds awarded through such grant for increasing research, education, technical, partnership, and innovation capacity, including for—

(1) building and upgrading institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities;

(2) building and upgrading institutional capacity to provide hands-on research and training experiences for undergraduate and graduate students; and

(3) outreach and recruitment to ensure students are aware of such new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities.

(f) REPORTING REQUIREMENTS.—Not later than—

(1) 1 year after the effective date of this section, as provided in subsection (h), and annually thereafter until the Director submits the report under paragraph (2), the Director shall prepare and submit to Congress a report on the status and progress of implementation of the grant program under this section, including on the number and nature of institutions participating, the number and nature of students served by institutions receiving grants, the level of funding provided to grant recipients, the types of activities being funded by the grants program, and plans for future implementation and development; and

(2) 5 years after the effective date of this section, as provided in subsection (h), the Director shall prepare and submit to Congress a report on the status of cybersecurity education programming and capacity-building at institutions receiving grants under this section, including changes in the scale and scope of these programs, associated facilities, or in accreditation status, and on the educational and employment outcomes of students participating in cybersecurity programs that have received support under this section.

(g) PERFORMANCE METRICS.—The Director shall establish performance metrics for grants awarded under this section.

(h) EFFECTIVE DATE.—This section shall take effect 1 year after the date of enactment of this Act.

SA 4786. Mr. MENENDEZ (for himself, Mr. SCHUMER, Mr. BOOKER, Mrs. GILLIBRAND, Mr. BLUMENTHAL, and Mr. MURPHY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. APPROPRIATIONS FOR CATCH-UP PAYMENTS.

Section 404(d)(4)(C) of the Justice for United States Victims of State Sponsored Terrorism Act (34 U.S.C. 20144(d)(4)(C)) is amended by adding at the end the following:

''(iv) FUNDING.—

''(I) APPROPRIATIONS.—

''(aa) IN GENERAL.—There are authorized to be appropriated and there are appropriated to the Fund such sums as may be necessary to carry out this subparagraph, to remain available until expended.

''(bb) EMERGENCY DESIGNATION.—The amounts provided under this subclause are designated as an emergency requirement pursuant to section 4(g) of the Statutory Pay-As-You-Go Act of 2010 (2 U.S.C. 933(g)).

''(cc) DESIGNATION IN THE HOUSE AND SENATE.—This subclause is designated by the Congress as being for an emergency requirement pursuant to section 4001(a)(1) and section 4001(b) of S. Con. Res. 14 (117th Congress), the concurrent resolution on the budget for fiscal year 2022.

''(II) LIMITATION.—Amounts appropriated pursuant to subclause (I) may not be used for a purpose other than to make lump sum catch-up payments under this subparagraph.''.

SA 4787. Mrs. SHAHEEN (for herself and Ms. COLLINS) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title VII, add the following:

Subtitle D—Access to Contraception

SEC. 761. SHORT TITLE.

This subtitle may be cited as the ''Access to Contraception for Servicemembers and Dependents Act of 2021''.

SEC. 762. FINDINGS.

Congress finds the following:

(1) Women are serving in the Armed Forces at increasing rates, playing a critical role in the national security of the United States. Women comprise more than 18 percent of members of the Armed Forces, and as of fiscal year 2019, more than 390,000 women serve on active duty in the Armed Forces or in the reserve components. An estimated several thousand transgender men also serve on active duty in the Armed Forces and in the reserve components, in addition to non-binary members and those who identify with a different gender.

(2) Ninety-five percent of women serving in the Armed Forces are of reproductive age and as of 2019, more than 700,000 female spouses and dependents of members of the Armed Forces on active duty are of reproductive age.

(3) The TRICARE program covered more than 1,570,000 women of reproductive age in 2019, including spouses and dependents of members of the Armed Forces on active duty. Additionally, thousands of transgender dependents of members of the Armed Forces are covered by the TRICARE program.

(4) The right to access contraception is grounded in the principle that contraception and the ability to determine if and when to have children are inextricably tied to one's wellbeing, equality, and ability to determine the course of one's life. These protections have helped access to contraception become a driving force in improving the health and financial security of individuals and their families.

(5) Access to contraception is critical to the health of every individual capable of becoming pregnant. This subtitle is intended to apply to all individuals with the capacity for pregnancy, including cisgender women, transgender men, non-binary individuals, those who identify with a different gender, and others.

(6) Studies have shown that when cost barriers to the full range of methods of contraception are eliminated, patients are more likely to use the contraceptive method that meets their needs, and therefore use contraception correctly and more consistently, reducing the risk of unintended pregnancy.

(7) Under the TRICARE program, members of the Armed Forces on active duty have full coverage of all prescription drugs, including contraception, without cost-sharing requirements, in line with the Patient Protection and Affordable Care Act (Public Law 111–148), which requires coverage of all contraceptive methods approved by the Food and Drug Administration for women and related services and education and counseling. However, members not on active duty and dependents of members do not have similar coverage of all methods of contraception approved by the Food and Drug Administration without cost-sharing when they obtain the contraceptive outside of a military medical treatment facility.

(8) In order to fill gaps in coverage and access to preventive care critical for women's